Headquarters
United States Army, Europe, and Seventh Army
United States Army Installation Management Agency
Europe Region Office
Heidelberg, Germany

Army in Europe
Pamphlet 25-25*

21 May 2004

Information Management

Army in Europe Information Technology Users Guide

***This pamphlet supersedes AE Pamphlet 25-25, 18 September 2003.**

For the CG, USAREUR/7A:

E. PEARSON
Colonel, GS
Deputy Chief of Staff

Official:

GARY C. MILLER
Regional Chief Information Officer - Europe

Summary. This pamphlet is a guide to using information technology (glossary) in the workplace. In support of information assurance, this guide prescribes procedures for using Government computers in a way that protects them against viruses and hackers.

Summary of Change. This revision incorporates new DOD and Army information assurance policy.

Applicability. This pamphlet applies to military and civilian personnel in the Army in Europe who use Government computers in the workplace.

Forms. AE and higher-level forms are available through the Army in Europe Publishing System (AEPUBS).

Records Management. Records created as a result of processes prescribed by this pamphlet must be identified, maintained, and disposed of according to AR 25-400-2. Record titles and descriptions are available on the Army Records Information Management System Web site at *https://www.arims.army.mil*.

Suggested Improvements. The proponent of this pamphlet is the USAREUR G6 (AEAIM-IAPM, DSN 380-5220). Users may suggest improvements to this pamphlet by sending DA Form 2028 to the USAREUR G6 (AEAIM-IAPM), Unit 29351, APO AE 09014-9351.

Distribution. A (AEPUBS).

CONTENTS

1. PURPOSE

a. As a user of a Government computer (GC), you can greatly affect the security of our networks. Protecting the information on those networks is called information assurance. This guide is your drivers manual for the information highway or “infobahn” and will help you do the right thing by showing you how to recognize and avoid the hazards awaiting you.

b. Before you can be issued a license to “drive,” you must take the Computer-User Test (para 7) and sign the Computer-User Agreement (app A). This agreement is your promise to use the network responsibly and to follow the command policy on computer use. This guide tells you everything you need to know to pass the test.

2. YOUR GOVERNMENT COMPUTER AS A GATEWAY TO INFORMATION AND THE INTERNET

a. Since almost all unclassified GCs in the Army in Europe are networked, your GC can reach or be reached by almost every unclassified GC in DOD. Because other DOD GCs trust your GC, you have access to DOD information not available to the general public. Additionally, almost all GCs on the LandWarNet (Unclas) are linked to the commercial Internet. The LandWarNet (Class), although not linked to the commercial Internet, is used to link DOD GCs together to share information classified up to Secret.

b. This internetworking of GCs makes your GC a gateway to vast amounts of information. It also exposes your GC to risks from all computers to which it can be linked. As a user of a GC in the Army in Europe, you play a key role in protecting our data.

3. WHAT IS THE THREAT?

Threats to your GC and networks in the Army in Europe can come from a virus, worm, hacker, or even from a soldier or DOD civilian in the military or U.S. Government.

a. Viruses and worms are programs that corrupt and damage programs, data, or both. A program does not have to perform malicious actions to be a virus or a worm; it only needs to infect or alter other programs. Most viruses, however, perform malicious actions, such as deleting data from your hard drive. Worms may manipulate a program on your GC that would allow a hacker free access to your data or use your computer as a “host” from which to infect other computers.

b. Opening an infected e-mail message or attachment from an unknown source is the most common method viruses are spread today. You should never configure your computer to automatically preview e-mail messages.

c. Virus-hoax warnings are more common than actual viruses. Many virus and e-mail hoaxes use fake technical or emotional language and include suggestions for “get-rich-quick” schemes or heart-rending pleas, such as an “urgent” warning to pass along information to protect everyone from a devastating virus.

d. Deliberately introducing “malicious logic” (the technical term for viruses and other malicious programs) into any Government information system is a violation of a lawful general order under the Uniform Code of Military Justice (UCMJ), Article 92. Personnel not subject to the UCMJ may be subject to adverse action under the United States Code, Federal regulations, or host-nation law. Hackers routinely attempt to exploit the security vulnerabilities found in the software you use to run your GC, often through the use of a virus or worm.

e. The best course of action is to prevent your GC from being infected in the first place. In the Army in Europe, there are five things users can do to ensure their GC and information are adequately protected:

- Ensure the anti-virus software on your GC is current. Army in Europe policy requires that your GC's anti-virus software be updated at least once a week. Anti-virus software must also be updated on all personal and Government-owned personal digital assistants (PDAs) and personal electronic devices (PEDs).

NOTE: In most organizations in the Army in Europe, anti-virus updates are automatically "pushed" to GCs. Soldiers and DOD civilians may also load a DOD anti-virus program on their home computers.

- The USAREUR Computer Security Baseline must be implemented and updated by your information management officer (IMO) or information assurance security officer (IASO).
- Be aware and report unusual computer activity (para 5).
- Log off your computer at the end of the day.
- Set your computer to scan "all files" when checking for viruses.

f. Even when taking the best precautions, viruses can still occur. They are not always immediately identifiable. Here are some things that may indicate the presence of a virus:

- Abnormal displays or banners appear on the computer screen.
- The computer's performance slows down.
- The computer shows unusual activity or displays error messages, file sizes change, or data or programs are lost.

4. USING YOUR GOVERNMENT COMPUTER

a. Safeguarding GCs.

(1) The GC you are using is the property of the U.S. Government. GCs are to be used by Government employees for official business, authorized personal use, and limited morale and welfare communications between deployed soldiers and their family members. All users must—

- Safeguard each information system and its information against sabotage, tampering, denial-of-service, espionage, and release to unauthorized persons.
- Protect hardware, software, and documentation at the highest classification of the information residing on the information system.
- Report information systems security incidents, vulnerabilities, and virus attacks to your system administrator (SA) or IASO.
- Check all magnetic media (for example, disks, compact disks (CDs), tapes, universal serial bus (USB) memory sticks) for malicious software (for example, viruses, worms) before using it on a GC, information technology (IT) system, or network in the Army in Europe.
- Check with your IASO to ensure that the system complies with the latest information assurance vulnerability alert (IAVA) (for example, when taking your laptop GC home for work or when returning from temporary duty).

(2) Soldiers who fail to comply with this policy may be subject to adverse administrative action or punishment under Article 92 of the UCMJ. Personnel not subject to the UCMJ may be subject to adverse action under the United States Code, Federal regulations, or host-nation law.

NOTE: Host-nation employees are not subject to the United States Code or Federal regulations. They are subject to host-nation laws.

b. Authorized Personal Use. Authorized personal use is defined by the Joint Ethics Regulation (JER) (DOD Reg 5500.7), paragraph 2-301; and AR 25-1. This use includes brief access to and searches on the Internet, and sending short e-mail messages. The JER also requires commanders and supervisors to ensure that personal use of GCs does not adversely affect the performance of official duties. Personal use of GCs is authorized when it—

- Conforms to DOD and Army in Europe policy.
- Is of reasonable duration and frequency and, when possible, is done before or after normal duty hours.
- Does not create significant additional costs to DOD or the Army, and does not reflect adversely on DOD or the Army.
- Serves a legitimate public interest, such as furthering the education and self-improvement of employees or improving employee morale and welfare. Employees may also be allowed to conduct job searches in response to downsizing. Using CGs to send e-mail between deployed soldiers and their immediate family members is authorized and strongly encouraged in the Army in Europe.

- Does not overburden the military communication system. Remember, the military communication system (of which the LandWarNet (Unclas) plays a vital part) is designed to support the mission requirements of the warfighter.

c. Passwords.

(1) Your password is your key to getting onto the information highway. While this key opens the vast world of various military networks and the Internet, it can also allow others access to the same information. As a GC user in the Army in Europe, you will have a unique log-on name and password for each GC account you use. Maintaining the security of your password is therefore one of the most important security precautions you must take as a user. You alone are responsible for protecting your password and any e-mail messages that originate from your account. If someone obtains your password, they could assume your identity in the virtual world. You are responsible for any activity that takes place on a GC under your log-on name and password. Do not share your password with anyone. The guidelines below will help you protect your password.

- Do not write down or post your password in your workarea.
- Do not store your password on-line or in a PDA or PED, and do not include it in e-mail messages.
- Make sure your password is not exposed on the screen when you log in.
- Ensure your password is changed every 150 days on the LandWarNet (Unclas) and every 90 days on the LandWarNet (Class). If you know that your password is compromised, report to your SA for a new one.
- If your account is on a classified network, your password is classified at the highest level of information on that network and you must protect it in the same manner as all classified information.

(2) Your password can be either user-generated or issued by your IMO. The following standards apply in the Army in Europe:

- **User-generated:** Passwords must have at least 10 characters and include at least 2 uppercase letters, 2 lowercase letters, 2 numbers, and 2 special characters. Passwords must not form a word or repeat any of your last 10 passwords. If your password does not meet current Army in Europe standards, you should inform your SA immediately.
- **IMO-generated and -issued:** Passwords must be random, 10-character, alphanumeric codes with at least 2 uppercase letters, 2 lowercase letters, 2 numbers, and 2 special characters.

(3) Never leave your GC unattended while logged on unless the GC is protected by a “password protected” screensaver.

d. Use of the LandWarNet (Class).

(1) Any computer connected to the LandWarNet (Class) (which is a classified network) operates in at least the U.S. Secret, “system-high” mode. Any magnetic media used on the system and printed output must be marked and controlled immediately according to AR 380-5 until the data is declassified or downgraded by an approved process. In other words, any disk going into a Secret system is now Secret and must be handled accordingly. A “Secret” label must be placed on write-protected media. Classified NATO material must be marked and controlled according to AR 380-15.

(2) You should not enter information into a system if the information—

(a) Has a higher classification than that for which the system is rated.

(b) Is proprietary, contractor-excluded, or otherwise needs special protection or handling.

(3) If a system is connected to the LandWarNet (Class), only U.S. personnel with a security clearance will be allowed unescorted access to the system. Magnetic disks or diskettes must not be removed from the computer area without the approval of the local commander or head of the organization. The IASO should inform you of TEMPEST requirements. TEMPEST (Red/Black) requires that system components be separated to prevent unauthorized monitoring. For this reason, the movement of hardware and other IT equipment must be approved by your IASO.

(4) Foreign national representatives will not have access to areas where LandWarNet (Class) equipment is located. If a foreign national representative is authorized access to a U.S.-controlled area, he or she must be announced and escorted at all times, and computer screens must be covered. If a foreign national representative is permitted to view a screen, U.S. personnel must ensure that the information viewed is releasable to that individual. At no time will a foreign national representative have control of a LandWarNet (Class) terminal.

(5) Unclassified information may be transferred from either the LandWarNet (Unclas) or LandWarNet (Class) using a procedure called air-gapping. See your IASO for approved procedures.

e. Use of Public Key Infrastructure Certificates. If you have a public key infrastructure (PKI) certificate installed on your computer (for example, software token), you are responsible for ensuring that it is removed when no longer required. If the certificate is no longer needed, you should notify your SA and the issuing trusted agent of local registration authority.

f. Authorized Software and Hardware. Software and hardware used on a GC must be licensed, accredited, and approved by your commander, IASO, and IMO. You should store original software in a secure location, such as a locked cabinet or drawer. You may not load any software on your GC or install or connect any hardware (including PDAs and PEDs, such as Palm Pilots) on a network in the Army in Europe without first obtaining written approval from your commander, IASO, SA, or IMO. Users should inform their IASO and SA of software requirements and obtain approval before installing software on a GC. Employee-owned IT (hardware and software) may be used to process Army-related work at the workplace provided the commander and the designated approving authority (DAA) for the network approve it. All PDAs and PEDs (personal or Government-owned) must be loaded with DOD-approved, anti-virus software.

g. Use of Army Knowledge Online (AKO). Soldiers, civilians, and contractors who are authorized e-mail accounts in the Army in Europe are required to have an AKO Web-mail account. All other Web-mail services are prohibited for Army business communications. AKO also provides the only authorized Internet chat service allowed on the LandWarNet (Unclas); all other chat services are prohibited. Management will provide host-nation civilians sponsorship for their AKO account.

h. Prohibited Web Sites. USAREUR has implemented WebSense, which is a program that blocks users from accessing prohibited Web sites (for example, those devoted to pornography and hate speech) and limits access for personal use. Authorized access may be obtained by exception. Contact your command IASO for assistance.

i. Prohibited Activity. As a user, you are the first line of defense against unauthorized computer activity. The JER and Army in Europe policy define prohibited computer software and computer-network misbehavior. The following is a summary (not prioritized) of this policy and prohibited activity on computer networks in the Army in Europe:

- Having or loading prohibited software onto GCs. Prohibited software includes peer-to-peer file-sharing software, such as MP3 music and video software; streaming audio and video; Moving Picture Experts Group (MPEG) files; hacker tools and development software; malicious logic and virus-development software, executables (files with an ".exe" extension), and macros; network line-monitoring and keystroke-monitoring tools; unlicensed (pirated) software; Web-page-altering software; games (including "America's Army"); personal firewalls (including DOD-licensed and Windows XP Internet connection firewalls); and any software not authorized by the unit commander and IMO.
- Using a commercial Internet chat service such as America Online (AOL) Instant Messenger, Yahoo Chat, and Web sites that promote chat services. AKO provides the only authorized chat service allowed on the LandWarNet (Unclas).
- Using networked IT or GCs for personal gain or illegal activities.
- Attempting to strain, test, circumvent, or bypass computer-network or security controls.
- Attempting to access data or use operating systems or programs, except as specifically authorized.
- Performing network line-monitoring or keystroke-monitoring without proper authorization.
- Modifying or tampering with the software or hardware on your GC without the approval of your SA, IASO, or IMO.
- Moving your GC without your SA, IASO or IMO's approval. Most damage to computers occurs when moving them.
- Introducing viruses, worms, or malicious codes into any IT or network.
- Sharing user-identification or passwords.
- Storing, processing, displaying, sending, or otherwise transmitting offensive or obscene material, such as racist, sexually explicit, harassing, or hate literature.
- Storing or processing classified information on a system (including PEDs and PDAs) not approved for classified processing.
- Storing or processing copyrighted material (including cartoons) unless approval is obtained from the author or publisher.
- Unauthorized viewing of; changing, damaging, or deleting; or blocking access to another user's files or communications.
- Obtaining, installing, copying, storing, or using software in violation of the appropriate vendor's license agreement.
- Giving an unauthorized individual access to a Government-owned or Government-operated system.
- Hacking into or from the USAREUR network.
- Sending or forwarding official e-mail from a GC connected to the LandWarNet (Unclas) to a commercial Internet service provider (ISP) (for example, AOL, CompuServe, Hotmail, Yahoo).
- Using someone else's user identification and password or masking your identity.
- Installing and using a modem without approval from your DAA.

- Writing or forwarding chain or hoax e-mail messages.
- Posting personal homepages.
- Using GCs for personal profit.
- Downloading or loading freeware or shareware software.
- Simultaneously connecting to a Government network and a commercial ISP.
- Simultaneously connecting to the LandWarNet (Unclas) and a commercial ISP with a PED or PDA modem.

j. Consent to Auditing and Monitoring.

(1) Auditing is defined as the independent review and examination of records and activities to assess the adequacy of system performance and controls, to ensure compliance with established policy and operational procedures, and to recommend necessary changes in controls, policy, or procedures. All transactions by users accessing the LandWarNet (Unclas) or LandWarNet (Class) are subject to audit.

(2) In general, Army members and employees use Government communications systems with the understanding that any type of use, authorized or unauthorized, incidental or personal, serves as consent to monitoring. When you click *OK* on the warning banner that appears when you start your GC, you are agreeing to have your GC monitored. GCs are monitored to ensure that use is authorized and that users follow security procedures. Among other things, monitoring is used for surveillance, to reconstruct account activity, and to record attempts to bypass security mechanisms.

k. Minimize Policy. During periods of heightened network activity, USAREUR may be forced to minimize non-mission-essential activity on our networks. When a *MINIMIZE* order is issued to all users of computer networks in the Army in Europe, all personal use of GCs is prohibited for the duration of the order, except for the following:

- E-mail messages between deployed soldiers and their families. Units are encouraged to make GCs available to family support groups for supervised use of Government networks to exchange e-mail with soldiers deployed in support of United Nations, NATO, and USEUCOM missions.
- GC use required for Army or other authorized education-center training or programs leading to college degrees.
- Morale, welfare, and recreation activities.
- Department of Defense Dependents Schools (DODDS) activities, provided student activity is monitored by adult supervisors.

5. REPORTING COMPUTER SECURITY INCIDENTS

a. If you think you have observed a computer security incident, you must report it to your SA or IASO immediately. A computer security incident is the act of violating an explicit or implied computer security policy. A few examples of computer security incidents are as follows:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data (for example, hacking).
- Attempts (either failed or successful) to defeat or circumvent computer-network or security controls (for example, WebSense, passwords).
- Downloading MP3 files or other unauthorized software.
- Writing or knowingly transmitting a virus, worm, or other form of malicious logic.
- Forwarding chain e-mail messages.

b. Additionally, immediately inform your SA or IASO if you think—

- Your GC has a virus.
- Your GC has been hacked or is being hacked.
- An authorized or required activity on the network is not functioning correctly.

c. If you believe your GC is infected with a virus or worm or is behaving strangely, immediately take the following steps:

- Do not turn off your GC.
- Disconnect the network cable from the GC (which looks like a telephone cable).
- Call your SA or IASO. If they are unavailable, call the Regional Computer Emergency Response Team, Europe (RCERT-E), hotline (DSN 380-5232).

6. HOW TO TREAT YOUR GOVERNMENT COMPUTER

You must treat your GC with care for it to function properly.

- Do not eat or drink near your GC. Spilling soft drinks, coffee, or other liquids on your GC can damage it and destroy your files.
- Keep your system clean and free of dust.
- Never disconnect your GC from its network-connection box (unless you think it is infected). The small network connections are very fragile and very expensive.
- Do not move your GC unless supervised by your SA or IASO.
- Turn your GC off at the end of the duty day unless you have been instructed by your SA or IMO to keep it on for IAVA updates. If your GC is turned off, it cannot be hacked. This also reduces the chance of fire.
- Do not expose your GC to extreme heat, cold, or humidity.

7. COMPUTER-USER TEST

a. Now that you have read and studied this guide, you are ready to take the Computer-User Test. To do so, log onto the Information Assurance Computer-User Test Web page at *https://www.uatp.hqusareur.army.mil*.

b. Once you have taken and passed the test, you will immediately receive an Information Assurance Computer-User License that authorizes you to drive on the USAREUR infobahn. Your license is valid for 3 years. If you are still driving on the infobahn after 3 years, you will be required to retake the Computer-User Test before you can renew your license.

c. Before you receive a log-on name and password for your GC, your IMO or IASO will require you to read and sign the Computer-User Agreement (app A). Your signature acknowledges your understanding of and agreement to support Army and Army in Europe policy on the use of GCs. Your signature also makes you accountable for every transaction that occurs on your GC account. If you refuse to sign, you will not be given an account for any computer network in the Army in Europe.

d. From the moment you log on, you will enjoy the benefits of driving on the infobahn, but you will also be faced with the responsibilities that come with it. There are hazards out there, and you are responsible for protecting your GC and your network from those hazards by following proper procedures. Remember, this guide is your “drivers manual.” Keep a copy near your computer or in one of your internal files.

8. CONCLUSION

As a GC user, you play a key role in protecting the integrity, availability, and confidentiality of data in the Army in Europe. Taking the steps listed above will help you ensure that your GC and all networks to which your GC is connected are safe. In doing so, you will not only be protecting yourself, you will be protecting the entire command. To summarize:

- Guard your password.
- Ensure your anti-virus software is up-to-date.
- Follow the rules on personal use of your computer.
- Report viruses and all other network-security incidents to your SA or IASO.

APPENDIX A
COMPUTER-USER AGREEMENT

This appendix is a copy of the Computer-User Agreement on the USAREUR Automation Training Program Web page at *https://www.uatp.hqusareur.army.mil*. Your system administrator (SA) or information assurance security officer (IASO) will ask you to sign a copy of this agreement before issuing you a password.

As a user of an information system in the Army in Europe, I will adhere to the following security rules:

1. I will use Army information systems (computers, systems, and networks) only for authorized purposes.

2. I will not import any Government-owned software or install hardware on any Government computer (GC) (for example, client-workstation, server) without first getting written approval from my commander, SA, or IASO.

3. I will not load any software onto my GC, Government information technology (IT) system, or network without the approval of my commander, SA, or IASO.

4. I will not try to access data or use operating systems or programs, except as specifically authorized.

5. I know I will be issued a user identification (user ID) and a password to authenticate my computer account. After receiving them—

a. I will not allow anyone else to have or use my password. If I know that my password is compromised, I will report to my SA for a new one.

b. If I have a classified account, I will ensure that my password is changed at least once every 90 days or if compromised, whichever is sooner.

c. If I have an unclassified account, I will ensure that my password is changed at least once every 150 days or if compromised, whichever is sooner.

d. If my account is on a classified network, I understand that my password is classified at the highest level of information on that network, and I will protect it in the same manner as that information.

e. I am responsible for all activity that occurs on my individual account once my password has been used to log on. If I am a member of a group account, I am responsible for all activity when I am logged on a system with that account.

f. I understand that if my password does not meet current Army in Europe standards, I am to inform my SA.

g. I will not store my password on any processor, microcomputer, personal digital assistant (PDA), personal electronic device (PED), or magnetic or electronic media.

h. I will not tamper with my GC to avoid adhering to Army in Europe password policy.

i. I will never leave my classified GC unattended while I am logged on unless the GC is protected by a “password protected” screensaver.

6. I know that it is a violation of policy for any computer user to try to mask or hide his or her identity, or to try to assume the identity of someone else.

7. I know that if connected to the LandWarNet (Class), my system operates at least in the U.S. Secret, “system-high” mode.

a. Any magnetic media used on the system must be marked and protected immediately according to AR 380-5. In other words, any disk going into a Secret system is now Secret and must be handled accordingly.

b. Magnetic disks or compact disks will not be removed from the computer area without the approval of the local commander or head of the organization.

c. I must protect all material printed out from the LandWarNet (Class) at the Secret level until the information is downgraded or declassified.

d. I will not enter information into a system if the information has a higher classification than that for which the system is accredited.

e. If connected to the LandWarNet (Class), only U.S. personnel with a security clearance are allowed unescorted access to the system.

f. Foreign military representatives will not have access to a LandWarNet (Class) terminal.

g. NATO material stored, processed, or transmitted on a LandWarNet (Class) terminal must be protected according to AR 380-15.

8. My local IASO has informed me of TEMPEST (Red/Black) separation requirements for system components, and I will ensure that those requirements are met. I will not move hardware or alter communications connections without first getting approval from the SA or IASO.

9. I will scan all magnetic media (for example, disks, CDs, tapes, universal serial bus (USB) memory sticks) for malicious software (for example, viruses, worms) before using it on a GC, IT system, or network in the Army in Europe.

10. I will use only approved methods to “air-gap” information from the LandWarNet (Unclas) or LandWarNet (Class).

11. I will not forward chain e-mail or virus warnings. I will report chain e-mail and virus warnings to my IASO and delete the message.

12. I will not run “sniffer” or any hacker-related software on my GC, Government IT system, or network.

13. I will not download file-sharing software (including MP3 music and video files) or games onto my GC, Government IT system, or network.

14. I will not connect any personal IT equipment (for example, PEDs and PDAs (such as Palm Pilots), personal computers, digitally enabled devices) to my GC or to any Government network without the written approval of my commander, SA, or IASO and IMO.

15. I will ensure that my anti-virus software on my GC is updated at least weekly.

16. I will not use Internet “chat” services (for example, America Online (AOL), Microsoft Network (MSN) Instant Messenger, Yahoo) from my GC. If chat service is needed, I will use my AKO account.

17. If I observe anything on the system I am using that indicates inadequate security, I will immediately notify the site IASO. I know what constitutes a security incident and know that I must immediately report such incidents to the IASO.

18. I will comply with security guidance issued by my SA and IASO.

19. If I have a public key infrastructure (PKI) certificate installed on my computer (for example, software token), I am responsible for ensuring that it is removed when no longer required. If the certificate is no longer needed, I will notify my SA and the issuing trusted agent of local registration authority.

20. I understand this agreement and will keep the system secure. If I am the site supervisor, group chief, SA, or IASO, I will ensure that all users in my area of responsibility sign this agreement.

21. I know I am subject to disciplinary action if I violate Army in Europe computer policy. For U.S. personnel, this means that if I fail to comply with this policy, I may be subject to adverse administrative action or punishment under Article 92 of the Uniform Code of Military Justice (UCMJ). If I am not subject to the UCMJ, I may be subject to adverse action under the United States Code, Federal regulations, or host-nation laws.

Computer-User Name (Typed or Printed):	_____	Security Officer Name (Typed or Printed):	_____
Computer-User Signature:	_____	Security Officer Signature:	_____
Date:	_____	Date:	_____

GLOSSARY

SECTION I
ABBREVIATIONS

AKO	Army Knowledge Online
AOL	America Online
CD	compact disk
DAA	designated approving authority
DOD	Department of Defense
GC	Government computer
IASO	information assurance security officer
IAVA	information assurance vulnerability alert
IMO	information management officer
ISP	Internet service provider
IT	information technology
JER	Joint Ethics Regulation
MPEG	Moving Picture Experts Group
NATO	North Atlantic Treaty Organization
PDA	personal digital assistant
PED	personal electronic device
PKI	public key infrastructure
SA	system administrator
UCMJ	Uniform Code of Military Justice
U.S.	United States
USAREUR	United States Army, Europe
USB	universal serial bus
USEUCOM	United States European Command

SECTION II
TERMS

information technology (IT)
The hardware, firmware, and software used as a part of an information system to perform DOD information functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment. IT includes any assembly of hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

LandWarNet (Class)
The name of the Army's classified network. This term replaced SIPRNET.

LandWarNet (Unclas)
The name of the Army's unclassified network. This term replaced NIPRNET.